Performances of Block Codes Attaining the Expurgated and Cutoff Rate Lower Bounds on the Error Exponent of Binary Classical-Quantum Channels

Pawel Wocjan, Dejan E. Lazic*, and Thomas Beth

Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe

Am Fasanengarten 5, D–76 131 Karlsruhe, Germany

*FZI Forschungszentrum Informatik,

Haid-und-Neu-Str. 10-14, D–76 131 Karlsruhe, Germany

February 1, 2008

Abstract

A conceptually simple method for derivation of lower bounds on the error exponent of specific families of block codes used on classical-quantum channels with arbitrary signal states over a finite Hilbert space is presented. It is shown that families of binary block codes with appropriately rescaled binomial multiplicity enumerators used on binary classical-quantum channels and decoded by the suboptimal decision rule introduced by Holevo attain the expurgated and cutoff rate lower bounds on the error exponent.

1 Introduction

In information theory the error exponent and its bounds, describing the exponential behavior of the decoding error probability, are important quantitive characteristics of channel performances. One can say that ever since Claude Shannon published his famous 1948 papers [1], information theorists mostly used and developed his *ensemble averaging* technique of obtaining an asymptotic in code length upper bound on the overall probability of block decoding error for the optimal channel block code. This central technique of information theory is usually referred to, not very appropriately, as "random coding" [2]. Formally, it consists of calculating the average probability of block decoding error over the ensemble of all sets of code words that are possible over the encoding space. This technique was adopted to *classical-quantum channels* in [3] [4] [5] [6] [7]. Especially, Holevo obtained the expurgated and cutoff rate lower bounds on the error exponent of classical-quantum channels with arbitrary signals states over a finite Hilbert space. The most unsatisfactory aspect of the ensemble

This paper has been presented at the Fifth International Conference on Quantum Communication Measurement & Computing Capri, Italy - July 3-8 2000.

averaging technique is that it can not determine the performance of a *specific familiy* of codes used on the channel considered, nor can it determine the requirements that a familiy of channel block codes should meet in order to attain the probability of error guaranteed by the channel error exponent or its lower bounds.

However, as shown in [8] for classical channels, it is possible to define error exponents and capacity measures for specific code families. In this paper we present a direct and conceptually simple method for derivation of lower bounds on the error exponent of specific families of block codes used on classical-quantum channels with arbitrary signal states over a finite Hilbert space. The (indirect) ensemble averaging technique uses the notion of an ensemble of all possible codes, thus concealing the requirements which a code family should meet, in order to have a positive error exponent and at best attain the channel error exponent. These requirements are now stated precisely by using the *method of multiplicity enumerators*. We show that families of binary block codes with appropriately *rescaled binomial multiplicity enumerators* attain the expurgated and cutoff rate lower bounds on the error exponent of binary classical-quantum channels even if decoded by a suboptimal decision rule introduced by Holevo.

The paper is organized as follows. In Section 2 we introduce the necessary definitions and notations to describe classical-quantum channels and give an overview of the results obtained so far by the ensemble averaging technique. In Section 3 the method of multiplicity enumerators is presented. Finally, in Section 3.1 and Section 3.2 we show that families of binary block codes with appropriately rescaled binomial multiplicity enumerators attain the expurgated and cutoff rate lower bounds on the error exponent of binary classical-quantum channels.

2 Classical-Quantum Channels

Let $\mathscr{C}$ denote a classical-quantum (c-q) channel [9] over a finite input alphabet $\mathscr{A} = \{a_1, \dots, a_q\}$, $|\mathscr{A}| = q\,(< \infty)$, with arbitrary channel output signal states $S_1, S_2, \dots, S_q$, given by density matrices over a finite dimensional Hilbert space. For an overview of other possible channel models arising in quantum information theory see [10].

A code word $\mathbf{x}_m = (x_{m1}, x_{m2}, \dots, x_{mN})$, $x_{mn} \in \mathscr{A}$, $m = 1, \dots, M$, transmitted over the channel $\mathscr{C}$ induces the product state $\mathbf{S}_m = S_{m1} \otimes S_{m2} \otimes \dots \otimes S_{mN}$ at the channel output. A *block code* $\mathscr{B}$ of length N and size $M \le q^N$ is a collection $\{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_M\}$ of M code words over $\mathscr{A}$ of length N, where $R = \log_2(M)/N$ is the *code rate* of $\mathscr{B}$. The quantum decoder for $\mathscr{B}$ used over $\mathscr{C}$ is statistically characterized by a *quantum decision rule* $\mathscr{D} = (\mathbf{D}_1, \mathbf{D}_2, \dots, \mathbf{D}_M)$ which is a collection of M *decision operators* satisfying $\sum_{m=1}^{M} \mathbf{D}_m \le I$.

Providing these operators a quantum decoder makes the measurement and the decision simultaneously, in contrast to a classical decoder which makes its decision on the already measured channel output [11] [12].

The conditional probability that the quantum decoder makes the decision in favor of the code word $\mathbf{x}_j$ when the code word $\mathbf{x}_m$ $(m \neq j)$ is transmitted over $\mathscr{C}$ is given by

$$e_m(\mathbf{x}_j) = \mathrm{Tr}\,\mathbf{S}_m \mathbf{D}_j\,, \tag{1}$$

where $\mathrm{Tr}(\cdot)$ denotes the trace of a matrix. The quantity $e_m(\mathbf{x}_j)$ is called the *error effect* of the code word $\mathbf{x}_j$ on the probability of erroneous decoding, P_{em}, of the transmitted

code word $\mathbf{x}_m$ [8]. Consequently the *word error probability* is given by

$$P_{\mathrm{em}} = P[\hat{\mathbf{x}} \neq \mathbf{x}_m \mid \mathbf{x}_m] = \sum_{\substack{j=1 \\ j\neq m}}^{M} e_m(\mathbf{x}_j)\,, \quad m = 1, \ldots, M, \tag{2}$$

where $\hat{\mathbf{x}}$ is the decision made by the rule $\mathscr{D}$. The *overall block decoding error probability*, P_{e}, can be expressed in the following form

$$P_{\mathrm{e}} = \sum_{m=1}^{M} P[\mathbf{x}_m] P_{\mathrm{em}} = \frac{1}{M}\sum_{m=1}^{M} P_{\mathrm{em}} = \frac{1}{M}\sum_{m=1}^{M}\sum_{\substack{j=1 \\ j\neq m}}^{M} e_m(\mathbf{x}_j)\,, \tag{3}$$

since all a priori code word probabilities $\{P[\mathbf{x}_m]\}_{m=1}^{M}$ are assumed to be equal which is the usual case in channel coding theory.

The design of a communication system for a channel $\mathscr{C}$ consits of the choice of the block code $\mathscr{B}$ and the decision rule $\mathscr{D}$. Once a code has been choosen, the *optimal decision rule* $\mathscr{D}_{\mathrm{opt}}$ minimizes P_{e} for this code. For all codes used on a memoryless classical channel the optimal decision rule is the *Maximum-likelihood* decoding. In general, the optimal decision rule on classical-quantum channels is not known [7]. However, conditions for the optimal quantum decision rule are given in [12] [13] [14].

For a given code length N and fixed code rate R there exists at least one *optimal block code* $\mathscr{B}_{\mathrm{opt}}$ producing the minimal overall block decoding error probability P_{eopt} on the channel $\mathscr{C}$, if decoded by the corresponding optimal decision rule $\mathscr{D}_{\mathrm{opt}}$.

2.1 Error Exponent

Asymptotic reliability performances (for $N \to \infty$) of the channel $\mathscr{C}$ can be expressed by the *reliability function* and the *channel capacity*. The reliability function, or *error exponent* [15], is given by

$$E(R) = \lim_{N\to\infty} \sup \left\{ -\frac{1}{N} \log_2[P_{\mathrm{eopt}}(R,N)] \right\}\,, \tag{4}$$

so that

$$P_{\mathrm{e}} \geq P_{\mathrm{eopt}}(R,N) = 2^{-N\cdot E(R)+o(N)}\,. \tag{5}$$

If the error exponent of the channel $\mathscr{C}$ has positive values, then the channel capacity R_c represents the largest code rate at which $E(R)$ is still positive. Otherwise the capacity of the channel is zero. For all code rates smaller than R_{c} there exists an infinite sequence of block codes and correponding decoding rules such that P_{e} decreases exponentially to zero (according to (5)) with $N \to \infty$.

The coding theorem determines the asymptotic reliability performances of the c-q channel and is composed of two parts: the direct part and the converse part. The direct part has been established in [3] [4] [5] by determining the c-q channel capacity as

$$R_{\mathrm{c}} = \max_{\mathbf{P}} \left[\mathrm{H}\left(\sum_{i=1}^{q} p_i S_i\right) - \sum_{i=1}^{q} p_i \mathrm{H}(S_i) \right]\,, \tag{6}$$

where the maximum is taken with respect to all a priori probability distributions $\mathbf{P} = (p_1, p_2, \ldots, p_q)$ on the input alphabet $\mathscr{A} = \{a_1, \ldots, a_q\}$, and $\mathrm{H}(S) = \mathrm{Tr}(S\log_2(S))$

denotes the von Neumann entropy. This result has been derived by the *random coding argument* [1] [16] [17] and the concept of *typical subspace* [18]. The weak converse of the channel coding theorem states that the overall block decoding error probability does not approach zero when the transmission rate is above the channel capacity R_{c}. Its proof [22] is based on the combination of the classical Fano's inequality and Holevo's upper bound [19] on the classical mutual information between the input and the output of a c-q channel followed by a quantum measurement. Holevo's bound can also be derived from the monotonicity of the quantum relative entropy [20] [21]. The *strong converse* of the coding theorem [23] states that the overall block decoding error probability increases exponentially with N up to one for any family of codes with rate R above the channel capacity R_{c}.

2.2 Random Coding Lower Bound

In [6] the *random coding exponent* $\underset{\sim}{E}_{\mathrm{r}}(R)$

$$\underset{\sim}{E}_{\mathrm{r}}(R) = \max_{0\leq s\leq 1} \max_{\mathbf{P}} [\mu(s, \mathbf{P}) - sR] \leq E(R) \tag{7}$$

has been conjectured as a lower bound on the error exponent of the c-q channel $\mathscr{C}$, where

$$\mu(\mathbf{P}, s) = -\log_2 \mathrm{Tr}\left[\left(\sum_{i=1}^{q} p_i S_i^{\frac{1}{1+s}}\right)^{1+s}\right], \tag{8}$$

and the second maximum in (7) is taken over all a priori probability distributions $\mathbf{P} = (p_1, p_2, \ldots, p_q)$ on the input alphabet $\mathscr{A} = \{a_1, \ldots, a_q\}$. The corresponding upper bound on the overall block decoding error probability is

$$P_{\mathrm{eopt}}(R, N) \leq a \cdot 2^{-N\cdot \underset{\sim}{E}_{\mathrm{r}}(R) + o(N)}, \tag{9}$$

where a is a positive constant.

For a *quasi-classical channel*, i.e. a c-q channel with commuting signal states S_i, the bound (7) is proved with $a = 1$ [15]. For a *pure state channel*, i.e. a channel with pure signal states S_i, the bounds (7) and (9) hold with $S_i^{1/(1+s)} = S_i$ (since each S_i is a projector) and $a = 2$ [6]. The proof of the random coding bound (7) in full generality, i.e. for c-q channels with arbitrary signal states S_i, remains an open question [7]. However, in this case the largest code rate R at which $\underset{\sim}{E}_{\mathrm{r}}(R)$ attains zero is equal to channel capacity given by (6) [7].

2.3 Suboptimal Decision Rule

In [7] the suboptimal decision rule $\mathscr{D}_{\mathcal{H}}$ has been introduced for any block code $\mathscr{B}$ used on the c-q channel $\mathscr{C}$ with arbitrary signal states S_i where

$$\mathscr{D}_{\mathcal{H}} = (\mathbf{D}_1, \mathbf{D}_2, \ldots, \mathbf{D}_M), \quad \mathbf{D}_m = \left(\sum_{j=1}^{M} \mathbf{S}_j^r\right)^{-\frac{1}{2}} \mathbf{S}_m^r \left(\sum_{j=1}^{M} \mathbf{S}_j^r\right)^{-\frac{1}{2}}, \tag{10}$$

$m = 1, 2\ldots, M$, and r can take any value from the interval $(0, 1]$. Furthermore, it has been shown that this decision rule produces a word error probability P_{em} upperbounded

by

$$P_{\text{em}} \leq \tilde{P}_{\text{em}} = \sum_{\substack{j=1 \\ j\neq m}}^{M} \operatorname{Tr} \mathbf{S}_m^{1-r} \mathbf{S}_j^r \,. \tag{11}$$

2.4 Cutoff Rate Lower Bound

By using the decision rule $\mathscr{D}_{\mathcal{H}}$ given by (10) with $r = \frac{1}{2}$ and the random coding argument the *cutoff rate lower bound* on the error exponent of the c-q channel $\mathscr{C}$

$$\underset{\sim}{E}_{\text{cut}}(R) = \max_{\mathbf{P}}[\mu(1, \mathbf{P})] - R \leq E(R)\,, \tag{12}$$

has been obtained [7].

The code rate R at which $\underset{\sim}{E}_{\text{cut}}(R)$ attains zero is the *quantum cutoff rate* [24], the quantum analogy of the classical cutoff rate [16]. It is given by

$$R_0 = \max_{\mathbf{P}} \mu(1, \mathbf{P}) = \max_{\mathbf{P}} \left\{ -\log_2 \operatorname{Tr} \left[\left(\sum_{i=1}^{q} p_i \sqrt{S_i} \right)^2 \right] \right\} , \tag{13}$$

and represents a lower bound on the channel capacity, i.e. $R_0 \leq R_{\text{c}}$ [7].

2.5 Expurgated Lower Bound

In [7] the *expurgated error exponent* $\underset{\sim}{E}_{ex}(R)$ as a lower bound on the error exponent

$$\underset{\sim}{E}_{\text{ex}}(R) = \max_{s\geq 1} \max_{\mathbf{P}}[\tilde{\mu}(\mathbf{P}, s) - sR] \leq E(R)\,, \tag{14}$$

has been obtained by expurgating poor code words from the codes in the ensemble [15]. The function $\tilde{\mu}(\mathbf{P}, s)$ in (14) is given by

$$\tilde{\mu}(\mathbf{P}, s) = -s \log_2 \left[\sum_{i,j=1}^{q} p_i p_j \left(\operatorname{Tr} \sqrt{S_i} \sqrt{S_j} \right)^{\frac{1}{s}} \right] . \tag{15}$$

The corresponding upper bound on the overall block decoding probability is given by

$$P_{\text{eopt}}(R, N) \leq 4 \cdot 2^{-N \cdot \underset{\sim}{E}_{\text{ex}}(R) + o(N)} \,. \tag{16}$$

2.6 Binary Classical-Quantum Channels

For binary c-q channels $\mathscr{C}$, i.e. channels over the input alphabet $\mathscr{A} = \{0, 1\}$ with the corresponding signal states S_1 and S_2, the expurgated and cutoff rate lower bounds can be computed explicitly. By introducing the channel parameter $c = \operatorname{Tr} \sqrt{S_1}\sqrt{S_2}$ of the binary c-q channel $\mathscr{C}$ the *cutoff rate lower bound* (12) can be expressed as

$$\underset{\sim}{E}_{\text{cut}}(R) = \max_{\mathbf{P}}[-\log_2(p^2 + (1-p)^2 + 2p(1-p)c) - R]\,, \tag{17}$$

and the *expurgated lower bound* (14) as

$$\underset{\sim}{E}_{\text{ex}}(R) = \max_{s\geq 1} \max_{\mathbf{P}}[-s \log_2(p^2 + (1-p)^2 + 2p(1-p)c^{\frac{1}{s}}) - sR]\,. \tag{18}$$

It is easily seen that in the binary case the cutoff rate lower bound and the expurgated lower bound are attained for the probability distribution $\mathbf{P} = (p = \frac{1}{2}, 1-p = \frac{1}{2})$. Consequently, the cutoff rate lower bound reduces to

$$\underset{\sim}{E}_{\text{cut}}(R) = R_0 - R \tag{19}$$

where R_0 is the cutoff rate given by

$$R_0 = 1 - \log_2(1+c)\,. \tag{20}$$

The expurgated lower bound is given by

$$\underset{\sim}{E}_{\text{ex}}(R) = \tilde{\mu}(\tilde{s}_R) - \tilde{s}_R R\,, \tag{21}$$

where $\tilde{\mu}(s) = \tilde{\mu}(\mathbf{P} = (\frac{1}{2}, \frac{1}{2}), s) = -s\log_2\left(\frac{1+c^{1/s}}{2}\right)$ and $\tilde{s}_R$ is implicitly given by $\frac{\partial}{\partial s}\tilde{\mu}(\tilde{s}_R) = R$. For rates below the *expurgated rate* R_{ex} given by

$$R_{\text{ex}} = \frac{\partial}{\partial s}\tilde{\mu}(1) = \tilde{\mu}(1) + \frac{c}{1+c}\log_2 c\,, \tag{22}$$

the expurgated lower bound is higher than the cutoff rate lower bound. For rates above the expurgated rate R_{ex} the expurgated and cutoff rate lower bounds coincide. These results have been obtained in [25] for the binary pure state channel. In this case the signal states are projectors $S_i = |\Psi_i\rangle\langle\Psi_i|$, for $i = 1, 2$, and the channel parameter is $c = \epsilon^2$ where $\epsilon = |\langle\Psi_1|\Psi_2\rangle|$.

3 Multiplicity Enumerators

In the following a binary c-q channel $\mathscr{C}$, i.e. a channel over the input alphabet $\mathscr{A} = \{0, 1\}$ with the corresponding signal states S_1 and S_2, will be considered. Over this channel binary codes $[N, R]$ of length N and code rate $R = \log_2(M)/N$ $(0 \le R \le 1)$ can be transmitted only.

Lemma 1 *The word error probability P_{em} of the code $[N, R]$ used on the channel $\mathscr{C}$ and decoded by the suboptimal decision rule (10) with $r = \frac{1}{2}$ is upperbounded by*

$$P_{\text{em}} \le \sum_{\substack{j=1\\ j\ne m}}^{M} 2^{-N[-\underline{\mathrm{d}}_{\mathrm{H}}(\mathbf{x}_m,\mathbf{x}_j)\log_2(c)]}\,, \tag{23}$$

where $c = \mathrm{Tr}\sqrt{S_1}\sqrt{S_2}$ and $\underline{\mathrm{d}}_{\mathrm{H}}(\mathbf{x}_m, \mathbf{x}_j) = \mathrm{d}_{\mathrm{H}}(\mathbf{x}_m, \mathbf{x}_j)/N$ is the normalized Hamming distance between the code words $\mathbf{x}_m$ and $\mathbf{x}_j$.

Proof: According to the decision rule $\mathscr{D}_{\mathcal{H}}$ given by (10) with $r = \frac{1}{2}$, for each pair of code words $\mathbf{x}_m$ and $\mathbf{x}_j$ $(j \ne m)$ in (11) holds

$$\mathrm{Tr}\sqrt{\mathbf{S}_m}\sqrt{\mathbf{S}_j} \quad = \quad \prod_{n=1}^{N}\mathrm{Tr}\sqrt{S_{mn}}\sqrt{S_{jn}} \tag{24}$$

$$
\begin{aligned}
&= \prod_{\substack{n=1\\ x_{mn}\neq x_{jn}}}^{N} \operatorname{Tr}\sqrt{S_{mn}}\sqrt{S_{jn}} && (25)\\
&= c^{\mathrm{d_H}(\mathbf{x}_m,\mathbf{x}_j)} && (26)\\
&= 2^{\mathrm{d_H}(\mathbf{x}_m,\mathbf{x}_j)\log_2(c)} && (27)\\
&= 2^{-N[-\underline{\mathrm{d}}_{\mathrm{H}}(\mathbf{x}_m,\mathbf{x}_j)\log_2(c)]}\,. && (28)
\end{aligned}
$$

By summing over all $j \neq m$ the proof is completed. □

Consequently, for the suboptimal decision rule $\mathscr{D}_{\mathcal{H}}$ given by (10) with $r = \frac{1}{2}$ the overall block decoding error probability is upperbounded by the *union bound* given by

$$
P_{\mathrm{e}} \leq \tilde{P}_{\mathrm{e}} = \frac{1}{M}\sum_{m=1}^{M}\sum_{\substack{j=1\\ j\neq m}}^{M} 2^{-N[-\underline{\mathrm{d}}_{\mathrm{H}}(\mathbf{x}_m,\mathbf{x}_j)\log_2(c)]}\,. \tag{29}
$$

On the classical binary symmetric channel (BSC) the union bound is also given by (29) but with $c = \sqrt{4p(1-p)}$, where p is the crossover probability.

The presented union bound on the overall block decoding error probability of a binary block code $[N, R]$ used on the c-q channel $\mathscr{C}$ and decoded by the suboptimal decision rule $\mathscr{D}_{\mathcal{H}}$ with $r = \frac{1}{2}$ depends on Hamming distances among the code words and the channel parameter c. This permits us to use a new method, derived from [8], in order to estimate the error exponent and the capacity performance of specific code families used on the c-q channel $\mathscr{C}$. For this purpose some necessary definitions and terms will be introduced.

Every code word $\mathbf{x}_m$ of a binary block code (linear or non-linear) $[N, R]$ has the Hamming *multiplicity enumerators* $\mathbf{M}_{\mathrm{H}}(\mathbf{x}_m)$ given by the $(N+1)$-tupel

$$
\mathbf{M}_{\mathrm{H}}(\mathbf{x}_m) = (M_{m0}, M_{m1}, \ldots, M_{mN})\,, \quad \sum_{n=0}^{N} M_{mn} = M\,, \tag{30}
$$

where M_{mn} represents the *multiplicity* (number) of code words on the Hamming distance n from the code word $\mathbf{x}_m$. The multiplicity M_{m0} is by definition equal to one.

The *average (expected) multiplicity enumerators* $\underline{\mathbf{M}}_{\mathrm{H}}[N, R]$ of the block code $[N, R]$ is given by

$$
\underline{\mathbf{M}}_{\mathrm{H}}[N, R] = (\underline{M}_0, \underline{M}_1, \ldots, \underline{M}_N)\,, \quad \sum_{n=0}^{N} \underline{M}_n = M\,, \tag{31}
$$

where

$$
\underline{M}_n = \mathrm{E}[\underline{M}_{mn}] = \frac{1}{M}\sum_{m=1}^{M} M_{mn} \tag{32}
$$

represents the average (expected) multiplicity of code words on the Hamming distance n.

The *weight enumerators* $\mathbf{W}_{\mathrm{H}}[N, R]$ of the block code $[N, R]$ is the $(N+1)$-tuple

$$
\mathbf{W}_{\mathrm{H}}[N, R] = (A_0, A_1, \ldots, A_N)\,, \quad \sum_{n=0}^{N} A_n = M\,, \tag{33}
$$

where A_n is the number of code words in $[N, R]$ of the Hamming weight equal to n. A_0 and A_N can take the values 0 or 1 only.

For linear codes the multiplicity enumerators of all code words are equal and coincide with the corresponding weight enumerators. For the non-redundant linear binary code of rate $R = 1$ ($M = 2^N$) weight enumerators (and multiplicity enumerators) are given by the corresponding binomial coefficients $\binom{N}{n}$, $n = 0, 1, \ldots, N$. Since

$$\sum_{n=0}^{N} \binom{N}{n} = 2^N , \tag{34}$$

it is obvious that there is no redundant binary block code $[N, R]$ ($R < 1$) with average multiplicity enumerators or weight enumerators given by all binomial coefficients $\binom{N}{n}$, $n = 0, 1, \ldots, N$. However, appropriately *rescaled binomial coefficients* $b\binom{N}{n}$, where $b = 2^{N(R-1)}$, satisfy the necessary condition

$$\sum_{n=0}^{N} b\binom{N}{n} = 2^{RN} = M , \tag{35}$$

for average multiplicity enumerators of redundant block codes.

For an infinite family of block codes *asymptotic performances* can be considered if the code length N of its members can tend to infinity. In general, this is the case for *fixed rate sequences*

$$\mathrm{FRS}(R) = \{[N_1, R], [N_2, R], \ldots, [N_i, R], \ldots\} \tag{36}$$

of block codes with the same code rate $R = \log_2(M_i)/N_i$ ($0 < R < 1$) and increasing code length, i.e. $N_i < N_{i+1}$ for $i = 1, 2, \ldots$.

In the asymptotic analysis of fixed rate sequences it is convenient to express the average multiplicities of the block code $[N_i, R] \in \mathrm{FSR}(R)$ by its *average multiplicity exponents* $\mathscr{M}_{\mathrm{H}}[N_i, R]$ given by the $(N_i + 1)$-tupel

$$\mathscr{M}_{\mathrm{H}}[N_i, R] = (\underline{\mathscr{M}}_0^{(i)}, \underline{\mathscr{M}}_1^{(i)}, \ldots, \underline{\mathscr{M}}_{N_i}^{(i)}) , \quad \sum_{n=0}^{N_i} 2^{N_i \underline{\mathscr{M}}_n^{(i)}} = M_i , \tag{37}$$

where

$$\underline{\mathscr{M}}_n^{(i)} = \frac{1}{N_i} \log_2(\underline{M}_n^{(i)}) , \quad n = 0, 1, \ldots, N_i \tag{38}$$

and $\underline{M}_n^{(i)}$ are given by (31). For $N_i \to \infty$ the corresponding asymptotic values (if they exist) form an infinite sequence representing the *asymptotic average multiplicity exponents* (AAME), $\mathscr{M}[R]_{\mathrm{FRS}}$, of the FSR$(R)$

$$\mathscr{M}[R]_{\mathrm{FRS}} = (\underline{\mathscr{M}}_0, \underline{\mathscr{M}}_1, \ldots, \underline{\mathscr{M}}_n, \ldots) \tag{39}$$

where

$$\underline{\mathscr{M}}_n = \lim_{N_i \to \infty} \frac{1}{N_i} \log_2(\underline{M}_n^{(i)}) , \quad n = 0, 1, 2, \ldots . \tag{40}$$

All possible values of the normalized Hamming distance $\underline{\mathrm{d}}_{\mathrm{H}} = \frac{n}{N_i}$ are in the interval $[0, 1]$ and in the asymptotic case the values

$$\underline{\delta}_{\mathrm{H}} = \lim_{N_i \to \infty} \left(\frac{n}{N_i} \right) \tag{41}$$

are dense enough. Consequently, the AAMEs can be replaced by a continous function, $\mathscr{M}(\underline{\delta}_{\mathrm{H}}, R)_{\mathrm{FRS}}$, which interpolates the discrete values of $\mathscr{M}_{\mathrm{H}}[R]_{\mathrm{FRS}}$. We will call this continous function of the continous argument $\underline{\delta}_{\mathrm{H}}$ and the parameter R the *interpolated asymptotic average multiplicity exponent* (IAAME) of the fixed rate sequence FRS(R) of block codes.

Lemma 2 *If the average multiplicity enumerators of the codes in the fixed rate sequence* FRS(R) *are given by rescaled binomial coefficients*

$$\left\{\underline{M}_n^{(i)} = \frac{a_i(n)}{2^{N_i(1-R)}}\binom{N_i}{n}\right\}_{n=0}^{N_i}, \quad \sum_{n=0}^{N_i} \underline{M}_n^{(i)} = M_i \tag{42}$$

where $a_i(n) = o(2^n)$, than the corresponding IAAME function is given by

$$\mathscr{M}(\underline{\delta}_{\mathrm{H}}, R)_{\mathrm{FRS}} = \mathrm{H}_2(\underline{\delta}_{\mathrm{H}}) - (1-R)\,, \tag{43}$$

where $\mathrm{H}_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ *represents the binary entropy function.*

Proof: By replacing (42) in (39) directly follows

$$\lim_{N_i\to\infty} \frac{1}{N_i}\log_2\left[\frac{a_i(n)}{2^{N_i(1-R)}}\binom{N_i}{n}\right], \quad n = 0, 1, \ldots, N_i\,. \tag{44}$$

Using the well known asymptotic relation (obtained from the Stirling approximation [26])

$$\lim_{N_i\to\infty}\binom{N_i}{n} = 2^{N_i\mathrm{H}_2(\frac{n}{N_i}) - o(N_i)}, \tag{45}$$

the limit (44) reduces to

$$\lim_{N_i\to\infty}\frac{\log_2(a_i(n))}{N_i} + \mathrm{H}_2(\underline{\delta}_{\mathrm{H}}) - (1-R)\,. \tag{46}$$

Taking into account the conditions on $a_i(n)$ and that $n \le N_i$ the limit in (46) tends to zero and the proof is completed. $\square$

Fixed rate sequences whose codes have average multiplicity enumerators are given by (42) will be called fixed rate sequences with *rescaled binomial average multiplicity enumerators.*

Consider an $[N, R]$ linear systematic binary block code with generator matrix $G = [I\,|\,A]$, where I is the $K\times K$ identity matrix ($K = RN$) and A is a $K\times(N-K)$ matrix of 0's and 1's. Suppose each entry of A is chosen at random, to be 0 or 1 with probability $\frac{1}{2}$, and then choose one of the codewords $\mathbf{x}$ at random. It is known [27] (Problems, pp. 287) that

$$\begin{aligned}&\mathrm{Prob}\{\mathrm{w_H}(\mathbf{x}) = 0\} = 2^{-K},\\ &\mathrm{Prob}\{\mathrm{w_H}(\mathbf{x}) = n\} = 2^{-N}\left\{\tbinom{N}{n} - \tbinom{N-K}{n}\right\},\ 0 < n \le N\,.\end{aligned} \tag{47}$$

The expected multiplicity enumerators of this random linear block code $[N, R]$ can be obtained by multiplying (47) with $M = 2^K = 2^{RN}$ for all codewords. Consequently, the IAAME function of a FSR(R) of these random linear block codes is given by (43).

Nonrandom linear binary block codes of finite length with average multiplicity enumerators closely fitting the rescaled binomial multiplicity enumerators have been found for $N \le 200$ in [28] [29].

3.1 Performances of binary block codes attaining the cut-off rate lower bound on the error exponent of a binary c-q channel

Theorem 1 (Cutoff rate lower bound) *Fixed rate sequences with rescaled binomial average multiplicity enumerators used on the binary c-q channel $\mathscr{C}$ and decoded by the suboptimal rule (10) with $r = \frac{1}{2}$ have an error exponent whose lower bound is the cutoff rate bound given by (19).*

Proof: Since all summands $2^{-N[-\underline{\mathrm{d}}_{\mathrm{H}}(\mathbf{x}_m,\mathbf{x}_j)\log_2(c)]}$ in (29) are equal for the same value of the normalized Hamming distance $\underline{\mathrm{d}}_{\mathrm{H}}(\mathbf{x}_m,\mathbf{x}_j)$, the overall block decoding error probability (3) can be upperbounded by

$$P_{\mathrm{e}} \leq \tilde{P}_{\mathrm{e}} = \sum_{n=0}^{N} \underline{M}_n 2^{-N[-\frac{n}{N}\log_2(c)]}\,,$$

where $\underline{M}_n$, $n = 0, 1, \ldots, N$, are the average multiplicities enumerators (31) of the code and $\frac{n}{N}$, $n = 0, 1, \ldots, N$ represent all possible values of the normalized Hamming distance $\underline{\mathrm{d}}_{\mathrm{H}}$. For codes from a fixed rate sequence (36) the average multiplicity exponents (37) can be used, so that

$$\begin{aligned} P_{\mathrm{e}}^{(i)} \leq \tilde{P}_{\mathrm{e}}^{(i)} &= \sum_{n=0}^{N_i} 2^{N_i \underline{\mathscr{M}}_n^{(i)}} 2^{-N_i[\frac{n}{N_i}\log_2(\frac{1}{c})]} \\ &= \sum_{n=0}^{N_i} 2^{-N_i[\frac{n}{N_i}\log_2(\frac{1}{c}) - \underline{\mathscr{M}}_n^{(i)}]}\,, \quad i = 0, 1, 2, \ldots\,. \end{aligned} \tag{48}$$

It is obvious that all the exponents in (48) should be negative for all permissible values of n and c, since otherwise the bound (48) becomes trivial, i.e. $P_{\mathrm{e}}^{(i)} \leq A$ with $A \geq 1$. Furthermore, if all exponents are negative, than the exponent with the minimal absolute value determines the upper bound if $N_i \to \infty$, so that

$$\tilde{P}_e^{(i)} = 2^{-N_i \min_{0\leq n\leq N_i}[\frac{n}{N_i}\log_2(\frac{1}{c}) - \underline{\mathscr{M}}_n^{(i)}] + o(N_i)} \geq P_{\mathrm{e}}^{(i)}\,.$$

By replacing the normalized Hamming distance $\frac{n}{N_i}$ by $\underline{\delta}_{\mathrm{H}}$ as in (41) and the AME $\underline{\mathscr{M}}_n^{(i)}$ by the IAAME $\underline{\mathscr{M}}(\underline{\delta}_{\mathrm{H}}, R)_{\mathrm{FSR}}$ given by (43), and comparing with (4) directly follows

$$\underset{\sim}{E}_{\mathrm{cut}}(R) = \min_{0\leq\underline{\delta}_{\mathrm{H}}\leq 1}[\underline{\delta}_{\mathrm{H}}\log_2\left(\frac{1}{c}\right) - \mathrm{H}_2(\underline{\delta}_{\mathrm{H}}) + 1 - R] \leq E(R)\,. \tag{49}$$

The function $\underline{\delta}_{\mathrm{H}}\log_2\left(\frac{1}{c}\right) - \mathrm{H}_2(\underline{\delta}_{\mathrm{H}}) + 1 - R$ has the minimum at

$$\underline{\delta}_{\mathrm{Heff}} = \frac{c}{1+c}\,. \tag{50}$$

This minimum is

$$\underset{\sim}{E}_{\mathrm{cut}}(R) = 1 - \log_2(1+c) - R\,, \tag{51}$$

so that the overall block decoding error probability decreases exponentially to zero for any code rate R below the cutoff rate R_0 given by (20). □

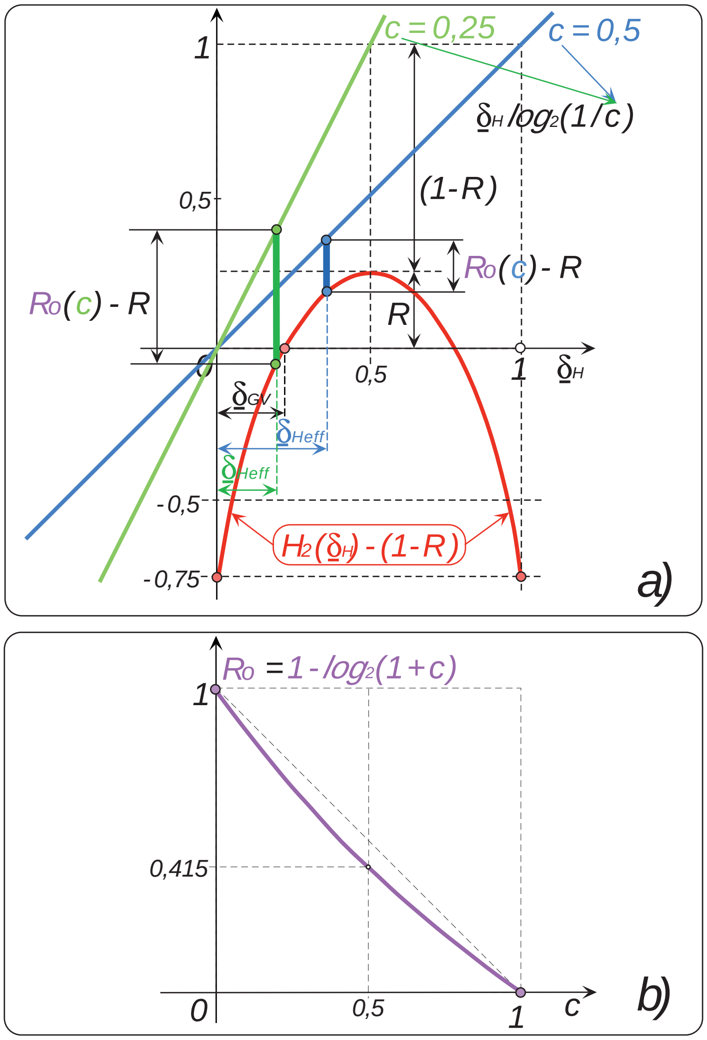

Figure 1: a) Graphical interpretation of the cutoff rate lower bound
b) Cutoff rate in dependence on the channel parameter c

Figure 1a gives the graphical interpretation of the method of multiplicity enumerators for obtaining the cutoff rate lower bound $\underset{\sim}{E}(R)_{\text{cut}}$ for fixed rate sequences of block codes $[N_i, R]$ with rescaled binomial multiplicity enumerators given by (42). The FSR(R) is characterized by its IAAME $\mathrm{H}_2(\underline{\delta}_\mathrm{H}) - (1-R)$. The suboptimal decoding rule (10) is characterized by the straight line passing through the origin with the slope $\log_2\left(\frac{1}{c}\right)$. The better the channel (i.e. the smaller c) the steeper is the slope of the straight line. This is illustrated by two values $c = 0.25$ and $c = 0.5$. The cutoff rate lower bound on the error exponent $\underset{\sim}{E}_{\text{cut}}(R)$ corresponds to the minimal vertical difference between the straight line characterizing the suboptimal decoding rule and the IAAME. The minimal difference is attained on the *effective Hamming distance* given by (50). In Figure 1b the dependence of the cutoff rate $R_0(c)$ on the channel parameter c is presented.
A very important consequence of Theorem 1 is that *only* code words on the effective Hamming distance (50) determine the cutoff rate lower bound. Note that this distance does not depend on the code rate. Generally, the effective Hamming distance is different

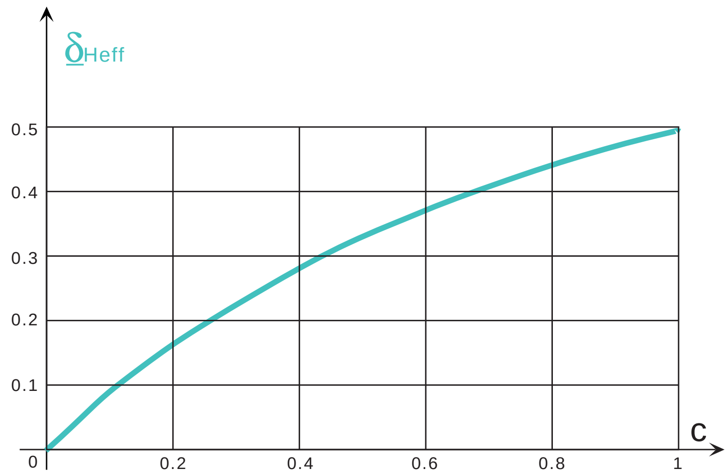

Figure 2: Effective distance in dependence on the channel parameter c

from the asymptotic *minimal Hamming distance* of the fixed rate sequence $\mathrm{FSR}(R)$ given by

$$\underset{\sim}{\delta}_{\min} = \lim_{N_i \to \infty} \frac{\mathrm{d}^{(i)}_{\mathrm{Hmin}}}{N_i}\,, \tag{52}$$

where

$$\mathrm{d}^{(i)}_{\mathrm{Hmin}} = \min\{\mathrm{d_H}(\mathbf{u}, \mathbf{v}) \mid \mathbf{u}, \mathbf{v} \in [N_i, R], \mathbf{u} \neq \mathbf{v}\}\,. \tag{53}$$

In Figure 2 the effective Hamming distance $\underset{\sim}{\delta}_{\mathrm{Heff}}$ in dependence on the channel parameter c is presented. The better the channel, the smaller is the effective Hamming distance $\underset{\sim}{\delta}_{\mathrm{Heff}}$. The worser the channel, the bigger is the effective distance and the minimal distance does not determine the cutoff rate lower bound if $\underset{\sim}{\delta}_{\min} < \underset{\sim}{\delta}_{\mathrm{Heff}}$.

It follows directly from (51) that a fixed rate sequence with rescaled binomial multiplicity enumerators used on the binary c-q channel and decoded by the suboptimal rule $\mathscr{D}_{\mathcal{H}}$, given by (10), with $r = \frac{1}{2}$ has a positive cutoff rate lower bound $\underset{\sim}{E}_{\mathrm{cut}}(R)$ if the channel parameter c satisfies

$$c \leq 2^{(1-R)} - 1\,. \tag{54}$$

3.2 Performances of binary block codes attaining the expurgated lower bound on the error exponent of a binary c-q channel

The *Gilbert-Varshamov lower bound* [27] on the asymptotic minimal normalized distance (52) of binary block codes $[N, R]$ is given by

$$\underset{\sim}{\delta}_{\mathrm{GV}}(R) = \mathrm{H}_2^{-1}(1-R)\,, \tag{55}$$

where H_2^{-1} denotes the inverse of the binary entropy function in the interval $[0, \frac{1}{2}]$. Thus, there exist fixed rate sequences $\mathrm{FSR}(R)$ such that the multiplicities of all code words $\mathbf{x}_m$, $m = 1, 2, \ldots, M^{(i)}$, satisfy

$$M^{(i)}_{mn} = 0\,, \tag{56}$$

for all Hamming distances n with $n \geq 1$ and $\frac{n}{N_i} \leq \underline{\delta}_{\mathrm{GV}}(R)$. Note that all fixed rate sequence with IAAMEs which have parts with negative values can be expurgated, i.e. it is possible to remove all code words which correspond to the negative parts of the IAAME without changing the code rate of the sequence in the asymptotic case ($N \to \infty$). Consequently, the IAAME of a FSR(R) with rescaled binomial multiplicity enumerators satisfying the Gilbert-Varshamov bound is given by the *expurgated IAAME*

$$\mathscr{M}(\underline{\delta}_{\mathrm{H}}, R)_{\mathrm{FSR}} = \begin{cases} -\infty & \text{for } \underline{\delta}_{\mathrm{H}} \leq \underline{\delta}_{\mathrm{GV}}\,, \\ \mathrm{H}_2(\underline{\delta}_{\mathrm{H}}) - (1-R) & \text{otherwise.} \end{cases} \tag{57}$$

Lemma 3 *Fixed rate sequences of linear block codes with rescaled binomial multiplicity enumerators (42) satisfy the Gilbert-Varshamov bound (55).*

Proof: The average multiplicites of linear codes coincide with the corresponding weight enumerators. The weight enumerators are natural numbers and cannot take values from the open intervall $(0, 1)$. Therefore the multiplicity exponents cannot be negative for linear codes. Consequently, fixed rate sequences of linear binary block codes with rescaled binomial average multiplicity enumerators (42) automatically satisfy the expurgated IAAME (57). □

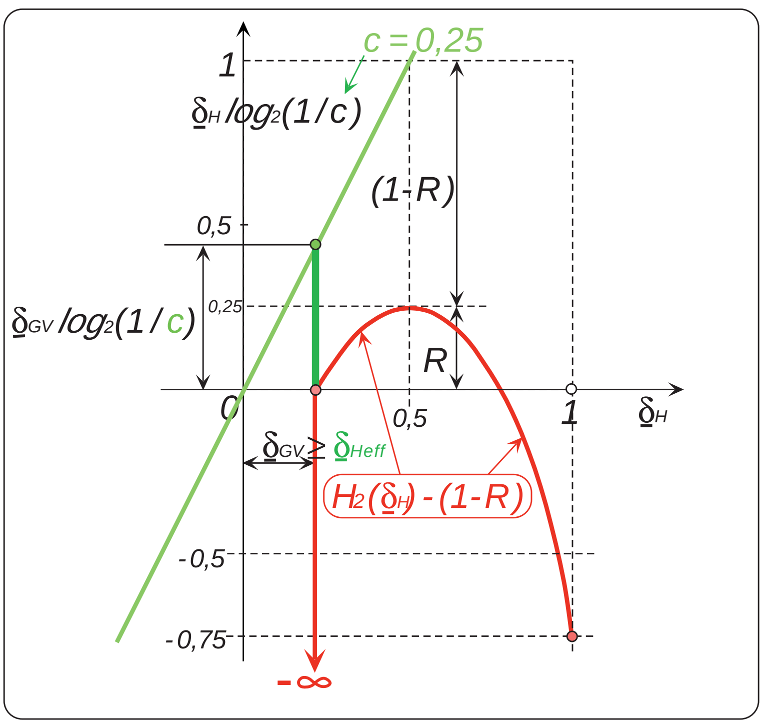

Figure 3: Graphical interpretation of the expurgated lower bound

Theorem 2 (Expurgated lower bound) *Fixed rate sequences with rescaled binomial multiplicity enumerators (42) satisfying the Gilbert-Varshamov bound (55) used*

on the binary c-q channel $\mathscr{C}$ and decoded by the suboptimal rule $\mathscr{D}_{\mathcal{H}}$, given by (10), with $r = \frac{1}{2}$ have an error exponent whose lower bound is the expurgated bound given by

$$\underset{\sim}{E}_{\mathrm{ex}}(R) = \log_2\left(\frac{1}{c}\right) \cdot \underline{\delta}_{\mathrm{GV}}(R) \tag{58}$$

for rates R below the expurgated rate R_{ex}

$$R_{\mathrm{ex}} = 1 - \mathrm{H}_2\left(\underline{\delta}_{\mathrm{Heff}}\right) \tag{59}$$

and the cutoff rate bound (19) for rates above R_{ex}.

Proof: The lower bound on the error exponent corresponds to the minimal vertical difference between the straight line $\underline{\delta}_{\mathrm{H}} \log_2\left(\frac{1}{c}\right)$ characterizing the suboptimal decoding rule (10) and the expurgated IAAME (57). It is clear (see Figure 3) that it can only be attained for $\underline{\delta}_{\mathrm{H}} \geq \underline{\delta}_{\mathrm{GV}}(R)$ since for $\underline{\delta}_{\mathrm{H}} < \underline{\delta}_{\mathrm{GV}}(R)$ the distance is infinite. Whenever the function $\underline{\delta}_{\mathrm{H}} \log_2\left(\frac{1}{c}\right) - \mathrm{H}_2(\underline{\delta}_{\mathrm{H}}) + 1 - R$ in Theorem 1 attains its minimum at $\underline{\delta}_{\mathrm{Heff}} \leq \underline{\delta}_{\mathrm{GV}}(R)$, or equivalently $R \leq R_{\mathrm{ex}} = 1 - \mathrm{H}_2\left(\underline{\delta}_{\mathrm{Heff}}\right)$, the lower bound on the error exponent is given by the expurgated error exponent (58). Otherwise the lower bound on the error exponent is given by the cutoff rate lower bound derived in Theorem 1. $\square$

The representation of the expurgated lower bound on the error exponent as $\underset{\sim}{E}_{\mathrm{ex}}(R) = \log_2\left(\frac{1}{c}\right) \cdot \underline{\delta}_{\mathrm{GV}}(R)$ is equivalent to (21). It can be recognized as the quantum analog of the *Gilbert-Varshamov Bhattacharyya distance* [8] [30] [31].

4 Conclusion

First we showed that the upper bound on the overall block decoding error probability of a binary block code $[N, R]$ used on a binary classical-quantum channel $\mathscr{C}$ and decoded by the suboptimal decision rule $\mathscr{D}_{\mathcal{H}}$ introduced by Holevo depends on the Hamming distances among the code words and the channel parameter c. This permited us to use the *method of multiplicity enumerators*, derived from [8], in order to estimate the error exponent and the capacity performance of a *specific code family* used on the c-q channel $\mathscr{C}$. We showed that the families of binary block codes with appropriately *rescaled binomial multiplicity enumerators* attain the expurgated and cutoff rate lower bound on the error exponent of binary classical-quantum channels with arbitrary signal states over a finite Hilbert space. The method of multiplicity enumerators provides a direct and conceptually simple method for derivation of these lower bounds.

For the classical binary symmetric channel is was shown in [28] that code families with rescaled binomial multiplicity enumerators attain the tight part of the random coding bound and thus the channel capacity. This was obtained by an improved upper-bounding of the decoding error probability assuming the Maximum-likelihood decoding. Unfortunately, this method cannot be applied directly to binary classical-quantum channels since the optimal decision rule for these channels is not known.

Acknowledgement

P. Wocjan is supported by Deutsche Forschungsgemeinschaft (DFG) "VIVA".

References

[1] C. E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J., Vol. 27, pp. 379–423 and 623–656, 1948.

[2] A. J. Viterbi, and J. K. Omura, *Principles of Digital Communication and Coding*, McGraw-Hill electrical enigeering series: Communications and information theory section, 1979.

[3] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, *Classical information capacity of a quantum channel*, Phys. Rev. A 54, pp. 1869–1876, 1996.

[4] B. Schumacher, and M. Westmoreland, *Sending classical information via noisy quantum channels*, Phys. Rev. A 56, pp. 132-138, 1997.

[5] A. S. Holevo, *The Capacity of the Quantum Channel with General Signal States*, IEEE Trans. Inform. Theory, Vol. 44, No. 1, January 1998.

[6] M. V. Burnashev, and A. S. Holevo, *On reliability function of quantum communication channel*, LANL preprint no. `quant-ph/9703013`.

[7] A. S. Holevo, *Reliability function of general classical-quantum channel*, LANL preprint no. `quant-ph/9907087`.

[8] D. E. Lazic, and V. Senk, *A Direct Geometrical Method for Bounding the Error Exponent for Any Specific Family of Channel Codes - Part I: Cutoff Rate Lower Bound for Block Codes*, IEEE Trans. Inform. Theory, Vol. 38, No. 4, pp. 1548–1559, September 1992.

[9] A. S. Holevo, *Problems in the mathematical theory of quantum communication channels*, Rep. Math. Phys., Vol. 12, No. 2, pp. 273–278, 1977.

[10] C. H. Bennett, and P. Shor, *Quantum Information Theory*, IEEE Trans. Inform. Theory, Vol. 44, No. 6, September 1998.

[11] K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory*. Lecture Notes in Physics, Vol. 190, Berlin: Springer-Verlag, 1983.

[12] C. H. Helstrom, *Quantum Detection and Estimation Theory*, Mathematics in Science and Engineering, Vol. 123, New York: Acedamic Press, 1976.

[13] A. S. Holevo, J. Multivariate. Anal. 3, pp. 337–394, (1973).

[14] H. P. Yuen, R. S. Kennedy, and M. Lax, *Optimal testing of multiple hypothesis in quantum detection theory*, IEEE, Trans., IT-21, pp. 125-134, 1975.

[15] R. G. Gallager, *Information Theory and Reliable Communication*, John Wiley and Sons, Inc., 1968.

[16] R. E. Blahut, *Principles and Practice of Information Theory*, Addison-Wesley, 1987.

[17] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, Inc., 1991.

[18] R. Josza, B. Schumacher, *A new proof of the quantum noiseless coding theorem*, J. Modern Optics, Vol. 41, pp. 2343–2349, 1994.

[19] A. S. Holevo, *Bounds for the quantity of information transmitted by a quantum communication channel*, Probl. Inform. Transm., Vol. 9, No. 3, pp. 177–183, 1973.

[20] G. Lindblad, *Completely positive maps and entropy inequalities*, Commun. Math. Phys., Vol. 40, pp. 147–151, 1975.

[21] A. Uhlmann, *Relative entropy and the Wigner-Yanse-Dyson-Lieb concavity in an interpolation theory*, Commun. Math. Phys., Vol. 54, pp. 21–32, 1977.

[22] A. S. Holevo, *On the capacity of quantum communication channel*, Probl. Inform. Transm., Vol. 15, No. 4, pp. 247–253, 1979.

[23] T. Ogawa, H. Nagaoka, *Strong Converse to the Quantum Channel Coding Theorem*, IEEE Trans. Inform. Theory, pp. 2486–2489, Vol. 45, No. 7, November 1999.

[24] M. Ban, K. Kurokawa, and O. Hirota, *Cutoff rate for quantum communication channels with entangled measurement*, Quantum and Semiclassical Optics, Vol. 44, L7–L12, 1998.

[25] A. S. Holevo, *Coding Theorems for Quantum Channels*, LANL preprint no. `quant-ph/9809023`.

[26] R. W. Hamming, *Coding and information theory*, Englewood Cliffs, NJ : Prentice-Hall, 1980.

[27] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Part I-II, North-Holland Publishing Company, 1977.

[28] Th. Beth, D. E. Lazic, and V. Senk, *A Family of Binary Codes with Asymptotically Good Distance Distribution*, Lecture Notes on Computer Science, 41, "EUROCODE", pp. 30–41, Springer, 1990.

[29] H. Kalouti, D. E. Lazic, and Th. Beth, *On the Relation Between Distance Distributions of Binary Block Codes and the Binomial Distribution*, Annales des Télécommunication, special issue on Channel Coding, Vol. 50, No. 9-10, pp. 762–778, 1995.

[30] J. K. Omura, *On general Gilbert bounds*, IEEE Trans. Inform. Theory, 15, pp. 661–665, 1973.

[31] J. K. Omura, *Expurgated Bounds, Bhattacharyya Distance, and Rate Distortion Function*, Information and Control, 24, pp. 358–383, 1974.